第1章

車載マイコンから機能安全まで，車載システム設計の基礎の基礎

――理解していますか？ 車載機器の使用環境と求められる信頼性

鈴村延保

ここでは，自動車のどのようなところが電子化されているかを見ながら，自動車を動かすコンピュータとその周辺に必須のセンサやアクチュエータの特徴を説明します．また，それらのコンピュータを実現するハードウェアやソフトウェアの特徴を理解するため，車載コンピュータの置かれている環境をまとめます．さらに，車載ソフトウェアの大規模化に伴う，設計や検証の効率化を考えるうえで重要になると思われるオブジェクト指向や機能安全規格「IEC61508」などについてお話しします．

（筆者）

「自動車はガソリンではなく，ソフトウェアで走るようになった！」．

最近，こんな比喩（ひゆ）も聞かれるくらい，自動車におけるソフトウェアの比重が大きくなっています．車両開発の80％にソフトウェアが関連する，とも言われています．新たな機能を創出するソフトウェアへの期待は非常に高まっており，メカにエレクトロニクスを組み合わせて新たな機能を創出する，かつての「メカトロニクス」と呼ばれた時代から，まさにソフトウェア＆メカトロニクスの時代へ突入したといえます（**図1**）．

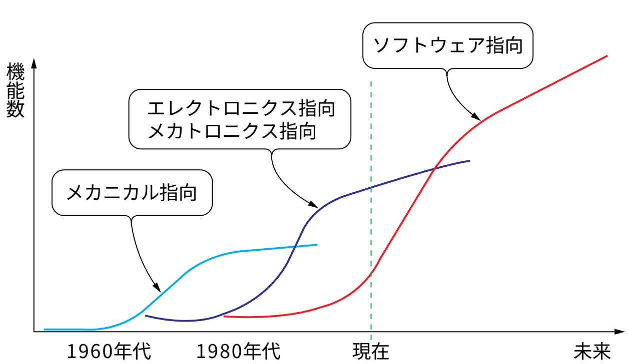


図1　高度な車両機能をソフトウェアで実現

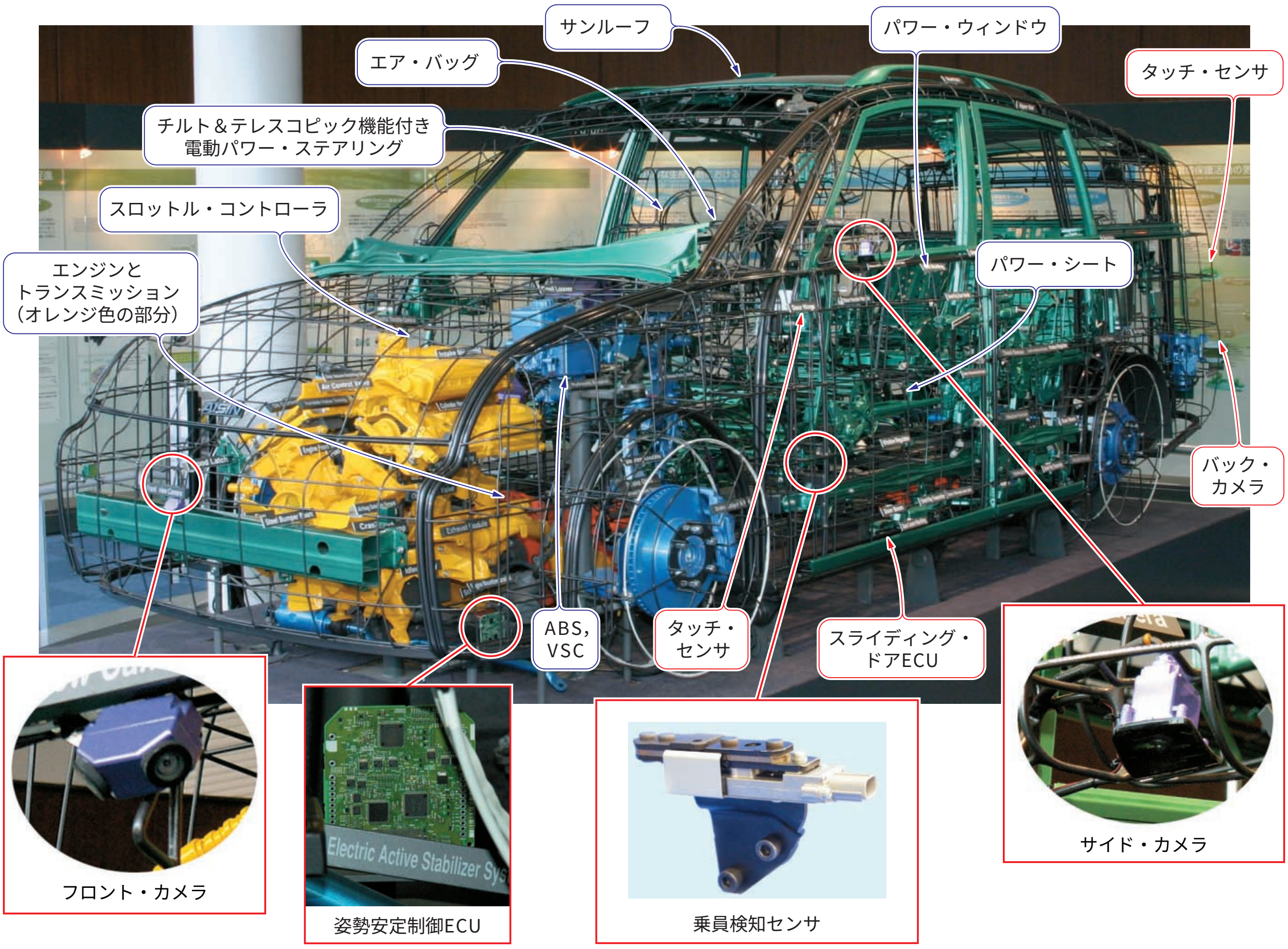
新たな機能を創出するために，自動車開発はソフトウェア＆メカトロニクスの時代に突入したといえる

1 「走る，曲がる，止まる」そして「人に地球にやさしく」

「自動車のすべての機能を実現するためにマイコンは不可欠になった」と言っても過言ではありません．では，具体的に自動車のどこにマイコンが使われているのでしょうか？ すぐに目に付くところでは，カー・ナビゲーション・システムやキーレス・エントリ，パワー・ウィンドウ，パワー・シートなどが挙げられます．このほかにも，エア・バッグやエンジン制御，姿勢制御（路面の状態に合わせてサスペンションを制御し，安定した走行を行えるようにする機能），ABS（anti-lock brake system），車線維持や車間距離制御などの運転者支援機能など，さまざまです．現在，マイコンを搭載した車載コンピュータ（ECU：electronic control unit）の数は，自動車1台当たり50個とも70個とも言われています（**写真1**，**図2**）．

「コンピュータ」といってもパソコンのような形はしていません．“弁当箱”と呼ばれる組み込みコンピュータらしいものから，一見機械部品と思われるメカ一体型，モータに内蔵されるようなインテリジェント・アクチュエータ型，センサに内蔵されるインテリジェント・センサ（スマ

KeyWord　ECU，スカイフック制御，アクチュエータ，MISRA-C，ADL，DSL，UML，フォーマル・メソッド，機能安全，IEC61508，ISO26262



▲写真1　進む自動車の電子化

走行制御だけでなく，安全性や利便性を向上させるためのさまざまな機能が自動車に搭載されている．こうした機能は複数のセンサと車載コンピュータで実現される．写真は，アイシン精機の製品や同社技術に関する展示を行っているアイシンコムセンター（愛知県刈谷市）に展示されているデモンストレーション・カー．自動車の内部のようすがわかる

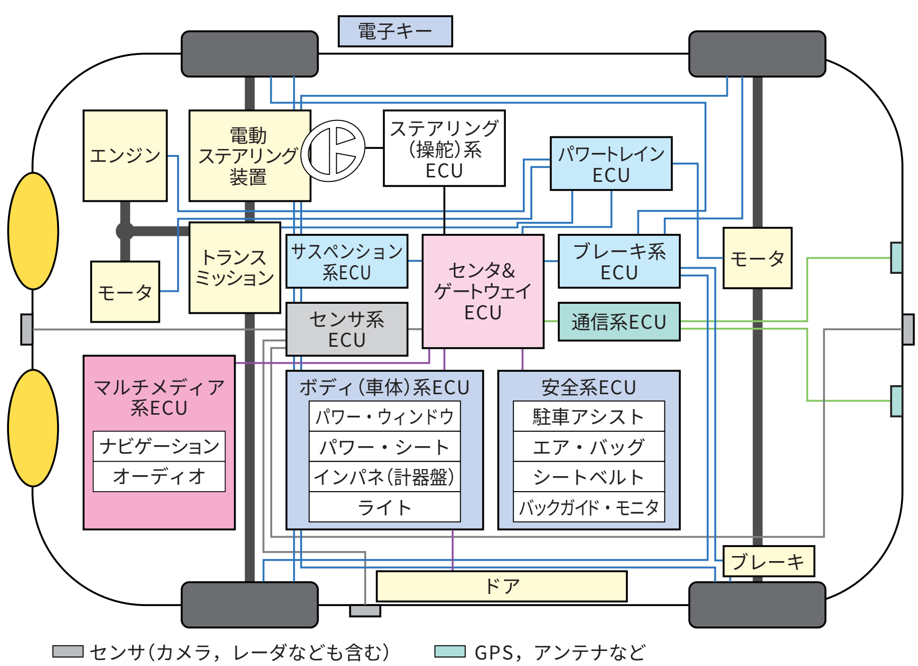


図2
車載コンピュータ（ECU）の構成例

現在，マイコンを搭載した車載コンピュータ（ECU）の数は，自動車1台当たり50個とも70個とも言われている

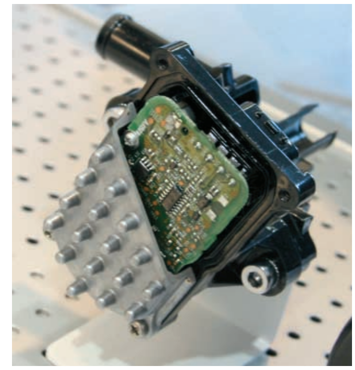
1



（a）弁当箱型ECU



（b）モーター一体型ECU



（c）アクチュエーター一体型ECU

写真2 各種車載コンピュータの例
(a)はマイコン・ボード型のECU，(b)はモータと一体になったECU，(c)はアクチュエーター一体型のECU．

ート・センサ）型など，さまざまな形で搭載されています（**写真2**）．

● クルマの基本「走る，曲がる，止まる」も電子化へ

例えば，走るためにはまずエンジンが必要です．エンジンといえば，昔はガソリンを供給する負圧吸引式キャブレタ，火花で燃料へ点火するケタリング式イグナイタ，遅角調整の負圧式ディストリビュータなどの部品から構成されていました．車好きの方には聞き慣れたことばだと思いますが，今では死語になりつつあります（p.28のコラム「システム開発者のためのメカ用語解説」を参照）．キャブレタはインジェクタと呼ばれるメカトロニクス部品に置き換わり，火花はディストリビュータのないフル・トランジスタ式イグナイタへと置き換わってきています．

また，変速機についてもかつての手動変速から自動変速のオートマチック・トランスミッション（AT）へと変化しました．初期のATは油圧式で，エンジン回転数を油圧ガバナで変速指令に利用していました．電子ATの時代になると，油圧をリニア・ソレノイドと呼ばれるアクチュエータを介して電気回路で変速制御するようになりました．

次に，曲がるためにはステアリング（操舵）装置が必要です．かつては重いハンドルを操作していたため，腕力の弱い人には自動車の運転に負担がかかりました．その後，油圧助勢によるステアリング装置となり，さらに現在では電気モータ助勢式に進化しました．

止まるためのブレーキでは，雪道などでタイヤのロックを防ぐABSが一般的です．

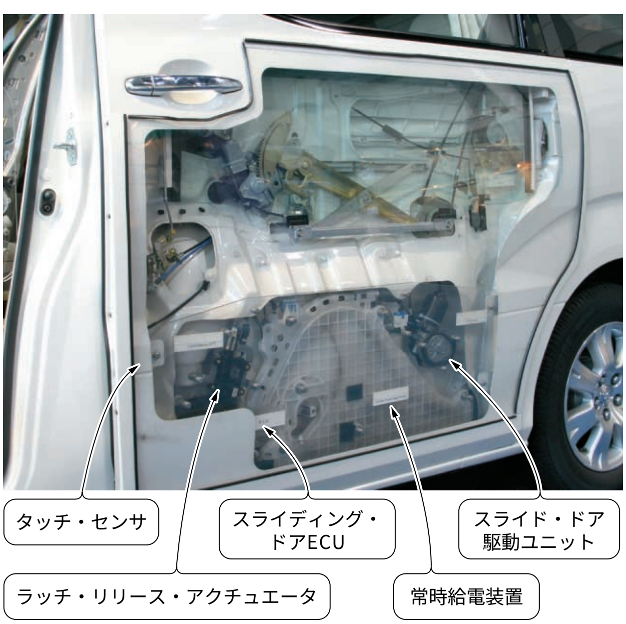


写真3 パワー・スライド・ドア・システムの例
運転席にあるスイッチやワイヤレス電子キーなどの操作でスライド・ドアの開閉を行えるシステム．挟み込み防止機能も搭載している

● 「安全，乗りごこち」の追求にはマイコン制御が必須

安全装置としては，エア・バッグ制御装置，追突防止装置などがあります．窓一つとっても，ただモータで上げ下げしているだけでなく，挟み込みを防止するための機能が搭載され，電子制御されています．

また，自動車の使い勝手や乗りごこちを向上させるための機能もたくさん備わってきています．ドアのロック/アンロック，サンルーフ，ワイパ，最近ではワンボックス・カーのスライド・ドアがボタン一つで作動します（**写真3**）．夜間のヘッドライト照灯は従来フィラメント式電球を用いていましたが，最近では昇圧された高電圧で発光するHID（high intensity discharge）と呼ばれるシステムに変わり，夜間でも明るく，かつ切れの良い灯火を実現しています．

乗りごこちを良くするには，自動車の姿勢を保つためにサスペンションやショック・アブソーバ，スタビライザ，車高調整装置などを用います（**写真4**）．それらもやはり電子制御化されており，たとえ路面に凸凹があっても空中からつり下げられているように車体の位置を固定する「スカイフック制御」が応用されています．

このように，マイコンで実現されている機能はまだまだきりがありません．最近では“by-wire”と呼ばれる，従来，飛行機などで利用されてきた技術や，ロボットなどで知られる画像認識，レーダ探査技術などの導入も進んでいます（**図3**）．

上述した動作を実現するため，モータだけでも100～200個使用されています．そのほか，油圧を調整するソレノイドも50個以上必要となります．電気モータとガソリン・エンジンで動くハイブリッド・カーでは，さらに多くの電子制御が行われています．一見鉄の塊に見える自動車ですが，電子関連部品は購入部品の半分を占める，とまで言われています．

また，最近ではECUを協調動作させる通信路が車両の中で神経のように広がっています．制御系のCAN（controller area network）やFlexRay，ボディ（車体）系のLIN（local interconnect network），エア・バッグ系のASRB（Automotive Safety Restraints Bus），情報系のMOST（Media Oriented Systems Transport）など，用途に応じた各種通信方式が用いられています．

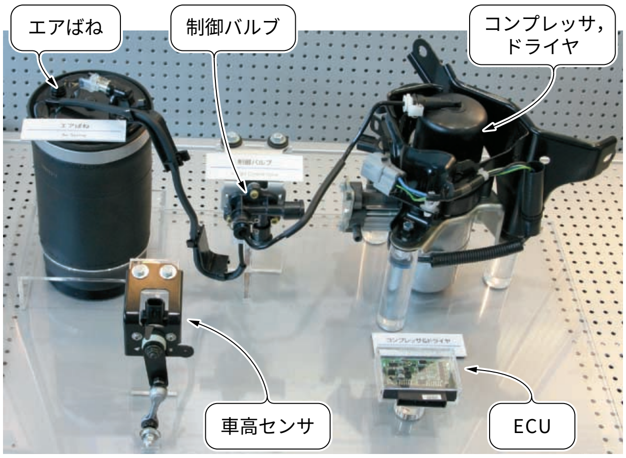


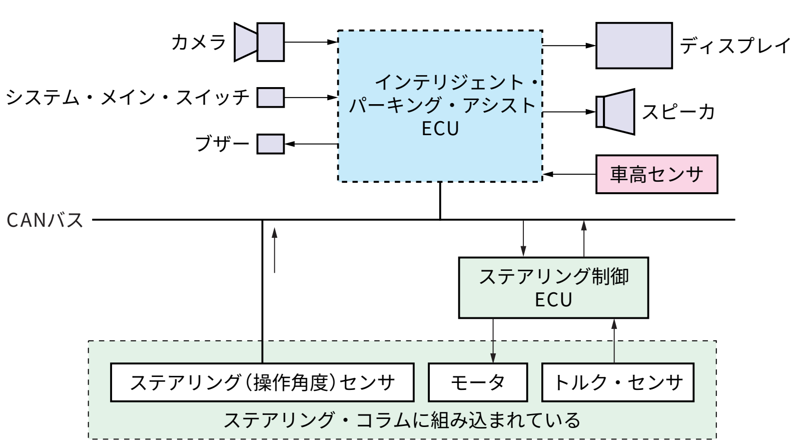
写真4　エア・サスペンション・システムの例

エア・サスペンション・システムにより，車両の姿勢が確保され，操縦の安定性が向上する．ECU，制御バルブ，コンプレッサ，およびドライヤ，車高センサなどから構成される

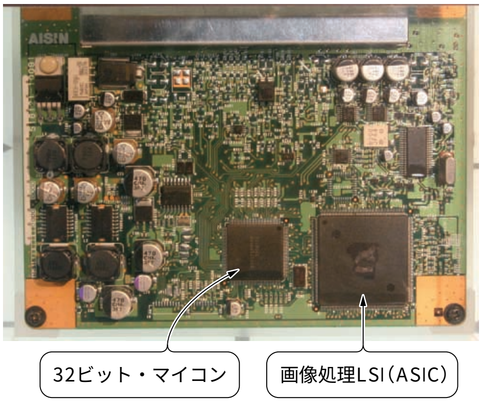
● コンピュータだけでは車は動かない

コンピュータが自動車のあちこちで活躍していることは理解していただけたと思いますが，コンピュータだけでは

1



（**a**）システム構成



（**b**）ECU



（**c**）ディスプレイの一例

図3　画像認識技術を用いた駐車支援システム

図は，アイシン精機とトヨタ自動車が共同開発した駐車支援システム「インテリジェントパーキングアシスト」．自動車後ろのナンバ・プレート付近に設置されているカメラを用いて，縦列駐車や車庫入れの際のステアリング操作を支援し，目標位置に導くシステム．本システムのECUには，32ビット・マイコンのほか，本システム専用に開発された画像処理LSIが搭載されている

あの重い自動車は動きません．

人間に例えて言うなら，頭脳にあたるコンピュータ（ECU），五感に相当する自動車の状況を感じ取るためのセンサ，手足相当の働きをするアクチュエータがそろって初めて自動車を制御することができます（図4，図5）．

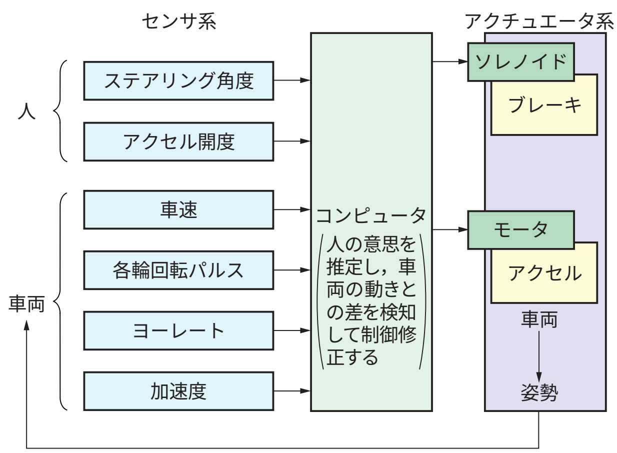


図5　入力構成の例

図は，車両安定制御システム（VSC：Vehicle Stability Control）におけるセンサ，コンピュータ，アクチュエータの関係を表したもの．VSCは，エンジンやブレーキを制御して横滑りを抑制し，車両の安定性を保つシステム．なお，VSCはトヨタ自動車の呼称である

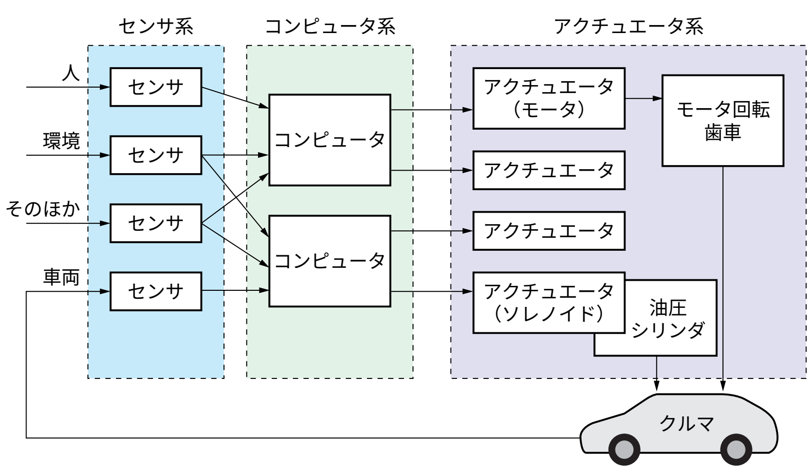
また，アクチュエータには車を動かすのにかなりの馬力が必要です．コンピュータで動かせるトランジスタやFETでは発熱の関係から，電流で数A（アンペア）くらいまでの制御が一般的でした．そのため，例えば油圧ポンプで蓄圧した油をソレノイド・バルブと呼ばれるアクチュエータを用いて調整し，てこの原理でピストンを押すなどして力を増幅して制御します．この点で，応答速度や作動音について設計時に苦労します．

2 車載ソフトウェアを取り巻く環境

車載マイコン・システム，いわゆるECUに実装されるソフトウェアの特徴を理解するには，そこに影響しているハードウェアだけでなく，それらを取り巻く環境にさかのぼって考える必要があります．

● ECUは高温，ノイズ，電磁波などにさらされている

車載コンピュータは以下の環境で動作しています．いず



（a）3要素の関係

方　式	種　類
空気圧式	●バキューム，正圧（バキューム・ポンプ），エンジンの負圧，エア・コンプレッサなどが必要 ●ON/OFFソレノイド・バルブ，デューティ制御バルブ，リニア・ソレノイド・バルブ
油圧式	油圧ポンプが必要
モータ式	●ブラシ・モータ：正転・逆転はリレーで制御．回転数制御はデューティやPWM（パルス幅）で制御 ●ステッピング・モータ ●ブラシレス3相モータ

（c）アクチュエータの機構の例

センサの種類	検出信号例
圧力	吸気，大気，油圧，乗員体重，ノッキング，タッチ・センサ，挟み込み，タイヤ空気圧
長さ，変移	車高，ブレーキ・ペダル，アクセル・ペダル，エンジン・スロットル，シート位置，ステアリング位置，燃料，オイル残量，トルク，アクチュエータ作動位置
温度	気温，水温，日射温，燃焼温度，排気ガス温度，油温
回転	車速，タイヤ回転，エンジン回転角度，変速機ギア回転，ステアリング角度
加速度	上下加速度，前後加速度，左右加速度，衝撃
ヨーレート（自転）	車両姿勢，走行距離
空気量	エンジン吸入空気
湿度	雨滴
化学物質	O_2，A/F（燃料空燃比）
電波	人近接，GPS位置情報，タイヤ空気圧信号
電圧	バッテリ電圧，アクチュエータ電圧，アクチュエータ電流
生体認証	表情，指紋，心拍
超音波，画像レーダ・レーザ	障害物，人，白線

（b）センサで検出する信号の例

図4　クルマを動かす3要素

自動車の状況を検知するセンサ，センサの情報から適切な制御を行うためのコンピュータ（ECU），コンピュータからの指令により実際に動力を生み出すアクチュエータの三つがそろって初めて自動車は動く

れも「そんなのあたりまえ」と思われることばかりですが，こうした環境の影響を受けていることをまず頭に入れておいてください．

● **自動車はバッテリで動作している**

バッテリの電圧変動が大きいため（10V～16V），動作電圧を補正する必要があります．また，自動車の始動時はバッテリ電圧が6V以下にまで下がるため，状況に応じて動作に配慮しなければなりません．最近ではハイパワーのモータ制御に伴い，42Vや288V以上の昇圧化など，電源が多種多様になっています．

● **自動車は世界中のあらゆる場所で使用される**

世界中で用いられるため，その環境温度範囲は－40℃～＋80℃（エンジン・ルームは100℃以上）と広いという特徴があります．半導体はもちろんのこと，温度によって作動させる油の粘度も大幅に違うため，アクチュエータなどでは動作温度を補正する必要があります．放送塔の近くなどへ移動すると車外電磁波の影響が大きくなります．この点にも考慮が必要です．

● **重い自動車を動かすため，油圧や大型モータのパワーを制御している**

適切な油圧制御を行うためには，あたりまえのことですが油圧特性を理解していなければなりません．油圧は配管の違いでも特性が違ってきます．大型モータについては作動ノイズが大きく，これがラジオ放送受信に影響を与えるため，ノイズを減らす制御も必要になります．

● **自動車には振動やノイズが多く，*S/N*が低い環境にある**

ランプやモータの突入電流によりグラウンド電圧が変動します．また，自動車はエンジンの燃料を点火するために強力な火花（イグニッション・パルス）を利用しています．センサ信号のA-D変換値にはイグニッション・ノイズが重畳しており，フィルタ技術（すなわち時間遅延）との戦いになります．また，カメラ画像について，昼と夜とでは明暗の差が激しく，処理が大きく異なってきます．

● **自動車は搭載場所が狭い**

電子化が進んでいるとはいっても，自動車の歴史の中から見ると電子部品は新参者です．そのため，電子部品を搭載するには新たな取り付け場所を見つける必要があります．携帯機器やそのほかの民生機器などと比べて自動車の体積は大きいので余裕があると思われるかもしれません．しかし，ボンネットの中などはエンジンや排気ガス管が通っていて，しかも高温であり，設置場所は限られます．アクチュエータも室内からあまり遠ざけるわけにも行かず，また作動音が乗員に聞こえてもいけないので，制御側でも静かさへの配慮が必要です．

注1：SAE（Society of Automotive Engineers；自動車技術会）の会議では，コンピュータに関連するセッションがある．以前はパワートレイン（Powertrain；エンジンと変速機）と排気ガス関連（Emission）が主だったが，現在はこのほか，安全性関連（Safety），高度車両制御技術関連（intelligent vehicle）に広がった．そのほか，ボディ系（Body Equipment），シャーシ制御（Chassis Control），ITS（Intelligent Vehicle Transport System）などの分野もある．

● 環境による制約を受けたマイコンで要求機能を実現

上記のような環境でECUが作動するため，使用する車載マイコンは，動作温度や電圧保証，ノイズ制約などから，民生機器市場向けのマイコンよりも動作周波数が低くなり，処理速度が低下します．こうした背景から，一般に車載ソフトウェアには**図6**に示すような特徴があります．車載ECUは分野（パワートレイン系，ボディ系，セーフティ系，情報系など）ごとにそれぞれ個性を持っているので，**図6**の特徴はあくまでも一般論としてとらえてください[注1]．

最近では，パラメータやテーブル・マップによる補間適合方法に限界が来ており，数学的モデルをシミュレーショ

- 時間制約が厳しく，時間のかかる演算を控えるくふう（苦労）が多い（固定小数点演算やテーブル演算の使用など）
- 電圧や温度の変動が大きいので，補正のため，テーブル補間やパラメータ調整が多い
- 油圧などは車両配管でも特性が変わるため，車両ごとのパラメータ調整を行いやすい配慮をする．
- ハイパワー制御が多い．そのため減速機構や油圧シリンダ利用し，応答速度が十分ではなく，予測制御など，制御遅延対策を施している．また，作動音について制御面での配慮を行っている．つまり，通常のフィードバック制御とフィードフォワード制御を組み合わせている．精度や応答改善のため学習制御が多用されている．
- 信号処理では *S/N* が悪いのでフィルタ処理が行われ，その制御遅延をどう挽回するか苦心している
- ロバスト（堅ろう性）ということばがよく使われる．例えば，A-D変換で通常想定する値の範囲を万が一超えたらどう処理するか，また各種トリガ信号の前後の微妙なずれなどを想定している
- 処理時間のワーストケースを明確にして設計を行う
- ウォッチドッグ機能によるソフトウェア監視など，ハードウェアとの連動監視を必要に応じて行っている
- システム異常でリセットすることが最適かどうかは，各システムによって異なる．マイコンだけでは対処できない場合，ハードウェアと協調して対応する
- センサの内蔵マイコンでは信号処理を重視（DSP的処理，テーブル補正処理，通信など）

図6　車載コンピュータのソフトウェアの特徴

動作温度や電圧保証，ノイズ制約などから車載ECUで用いるマイコンは民生機器向けのものと比べて，動作周波数が低い．こうした背景から，一般に図のような車載ソフトウェアの特徴が挙げられる

ンし，パラメータを推定して制御に応用しています．車両ごとに微妙にソフトウェアが異なることから，効率的なソフトウェア構築方法として，ソフトウェア・プロダクト・ライン（SPL：software product line）が注目されています．

25年前，世界初のマイコン式自動変速機は4ビット・マイコンで制御され，ROM容量はほんの2Kバイト（アセンブラで2,000行以下）でした．現代では，車載マイコンは32ビットがあたりまえで，車両全体のソフトウェアの量はC言語で数百万行と言われます．このことは，図1でも示しましたが，ソフトウェアが自動車を革新するブレークスルーとなる期待の表れです．

● 動作温度や精度だけではない車載マイコンへの要望

1970年代，最初に自動車に搭載されたマイコンは，Misarと呼ばれるカスタムの12ビット・マイコンでした．このようなマイコンが使われたのは，自動車制御では演算精度が必要であるため，そして，動作環境や信頼性などが民生機器市場と異なった特殊性があるためでした．

ここまでに説明したように，現在では自動車のどこを見ても（センサの中でさえ）マイコンが搭載されています．そのため，マイコンへの要求は単に精度が高いとか信頼性が高いというだけでなく，もっと広範なものになっています（図7）．

- ECUに使用するマイコンはローエンド（8ビット）からハイエンド（32ビット以上）までと広範囲
- ハイエンド品は速ければ速いほど，やりたいこと（機能）が実現できる
- Mバイト・オーダのROM，数百Kバイト・オーダのRAMを内蔵した1チップ・マイコン
- 多チャネルのA-Dコンバータ（かつて8チャネルが一般的仕様であった時期に24チャネルが出現）
- 不揮発RAM搭載
- 待機時の低消費電力化に対応（スタンバイ・モードや低消費電力動作モード）
- 開発短期化へ対応できるオンボードで書き換え可能なフラッシュ・メモリの内蔵
- 小型，高集積．CSP（chip size package）やMCM（マルチチップ・モジュール）実装の採用
- 車載固有の通信ポート（CAN，LIN，FlexRay，ASRB，MOSTなど）の搭載
- IDB（ITS/international data bus），NBD（Non Break Debug）などのデバッグ・ポートを搭載．USBのような高速で少ピン数のシリアル・ポートだとさらに良い．CANなどで代用する場合は複数チャネルが必要
- 発生ノイズを低く抑える
- 外乱ノイズや電源変動に強い
- 低消費電力
- エンジン・ルーム搭載用などでは120℃以上の環境で動作を保証
- 10年〜15年という長期間の供給
- 周辺ICなどとのインターフェースの容易さ（内部3.3V動作でもI/O電圧は5V）
- 豊富な故障診断機能

図7　車載用マイコンへの主要な要望

自動車のさまざまな機能を実現しているため，車載用マイコンへの要求も多岐にわたる

また，最近はソフトウェアの大規模化に伴い，一つのマイコンに各種の異なったシステム制御ソフトウェアを同居させる統合制御が広く利用されています．このような場合，制御を効率的に統括するリアルタイムOS（車載ではOSEK/VDXが主流）が搭載されます．ハード・リアルタイムと呼ばれる，時間制約の厳しい自動車制御を安全に統合するには，従来のメモリ保護に加え，新たに時間保護機能を効率的に実行するマイコンの登場が期待されています．

これらを含めて，現在，機能安全（詳細は後述）という考えかたが浸透してきています．今後，車両制御のどういった部分を担うかによって，故障診断機能や冗長機能などについてのマイコンへの要求がグローバルな基準で規定されるようになると予想されています．

3　車載ソフトウェア開発の実際

現在，車載ソフトウェア開発はほとんどがC言語で行われています．これは，オブジェクト生成効率の良いマイコンとコンパイラの出現が寄与していますが，むしろ開発効率が重視されているからといえます．開発効率の観点からいうと，高級言語の持つ高い生産性や再利用性という長所はもちろんですが，標準言語を利用することによる支援ツールの恩恵が重視されています．具体的には，ソース・コードを静的，動的に解析してレビューしたり，シミュレーションを利用して検証を行うなど，各種ツールを組み合わせて開発環境を構築できる点です．

一方，C言語は「どんなふうにでも書ける」という点が問題となります．紛らわしい表現を避ける意味で，MISRA-C（正式名称は“Guidelines for the Use of the C Language in Vehicle Based Software”）というコーディング規約が自動車分野で提唱され，普及しています．

● 「デバッグ済み」はどのレベルの検証を意味するか

車載ソフトウェアだから特殊というわけではありませんが，ICE（in-circuit emulator）によるブレーク・ポイント・デバッグだと，どうしても関数単位の検証になるので，

動作させたままのデバッグというわけにはいきません．

制御ソフトウェアはフィードバック制御などを行っており，実際に動いた状況でないと仕様上検証できない点があります．そのため，テスト・コースで車を走らせてソフトウェア動作を内部モニタして確認したり，実験室でできるだけ車の動きを模擬したりします．

実車の動作を模擬する場合，次のような手法をとります．

- **HILS（Hardware In the Loop System）**――ECU（ソフトウェアも含む）は実機で，車など，その周辺機械はコンピュータなどによる模擬環境
- **SILS（Software In the Loop System）**――ECUも模擬環境（ソフトウェアだけ実物）．ハードウェアが準備できていなくてもテストが進められるが，処理速度が遅い
- **PILS（Processor In the Loop System）**――マイコンだけ実機という模擬環境．I/Oドライバ・ソフトウェアにパッチを当てて，模擬環境と接続する

民生機器ではマイコンは「仕様書どおりに動くもの」ということで，SILSやHILSを実施すれば「デバッグした」と言えると思います．自動車の場合，マイコンの微妙な動作まで考慮する場合もあり，そういうときはPILSという手法を使います．

実車による評価となると，それはデバッグ機器でも極寒（－30℃）および酷暑（80℃）で動作する必要があります．マイコンの評価ボードではフラット・ケーブルなどは接触不良の問題から使いにくく，ピン数の少ないバスやデバッグ機能を内蔵した1チップ・マイコンが要求されます．

● 車載ソフトウェア開発もオブジェクト指向へ？

ソフトウェアの大規模化に伴い，民生機器の市場ではC++やJavaなどのオブジェクト指向言語が活用されています．

車載ソフトウェア，その中でもとくに制御系では，ワーストケース処理時間（WCET）が重視されることから，動的メモリ配置を行う言語の活用は進んでいません．しかし，オブジェクト指向は利用されないかというとそういうわけではなく，発想を具体化する手段として活用されてきています．生産性を補う方向としては，モデリング記述（モデル・ベース設計：MBD）でC言語を包み込むようになっています．

● ヘテロジニアス，ハイブリッド，アーキテクチャ重視

ソフトウェアの世界でモデル・ベース設計というと，UML（unified modeling language）が有名ですが，自動車制御分野ではMATLAB/Simulinkがよく活用されています．この理由として，UMLは次の二つの点が弱いことが挙げられています．

一つは，UMLはシステム記述言語とは言われていますが，いわゆるESL（electronic system level）からスタートしています．自動車のように，ハードウェアとソフトウェアだけでなく，メカや油圧など，ヘテロジニアス（異種混合）な要素でシステムが構成されている場合，UMLによる統一記述は難しいのです．また，値の取り扱いについても，ディスクリート値（状態遷移図などを連想してほしい）には強いが，電流などのリニア値を使ったフィードバック制御記述などには弱いといえます（両方の値を扱うモデルをハイブリッド・モデルと呼ぶ）．

蛇足ですが，ハードウェアとソフトウェアが中心となるエレクトロニクスの世界では，「システム記述言語のC」などと言われるように，システムということばはハードウェア要素とソフトウェア要素が中心となって議論されます．しかし，その場合のシステムとは，実はESLのシステムを言っており，自動車分野から見ると「あれっ？」と感じる場面が少なからずあります．自動車制御では「システム」というと，「メカの動作や油圧などを含めた，もう一段上までのヘテロジニアスな要素で構成されたシステム」を意味します．つまり，フィードバック制御を行うので，その系に含まれる要素がシステム構成要素になるわけです．

UMLのもう一つの弱点は，よりソフトウェア実装に近い構成モデルの記述です．具体的には，ポート，コネクタといった，インターフェースのイメージが記述しにくい点が挙げられます．このことは，「アーキテクチャ・レベルの記述が弱い」とも言えます．ただし，UML 2.0ではこの点が改良されてきています．この考えかたはADL（Architecture Description Language）概念と定義され，組み込みソフトウェアを部品化して扱う場合に重要です．なお，ADL概念はUMLと同時期のここ10年で定義が形式化され，進展しています．

UMLはISO規格化されてグローバル標準になっていくことから，応用の拡大が期待されています．しかし，今後のUMLの改良ですべての要望に対応することは難しいでしょう．そのため，ドメイン単位（例えば自動車制御と

いうドメイン）でUMLの拡張メカニズムを利用したDSL（Domain Specific Language）を策定し，利用していくという流れがあります．また，目的に合ったモデリング言語を機能開発単位で利用し，ソフトウェア部品化して，アーキテクチャ・レベルで組み合わせて再利用します．

オブジェクト指向では，再利用はクラス図やクラス・パターンで検討されますが，先に述べたワーストケース処理時間の把握しやすさなどを考慮すると，車載組み込みソフトウェア開発はちょっと違った方向となります．

● 実装と検証の効率化＝ソフトウェアの部品化・再利用化

大規模ソフトウェアとなると，そのワーストケース処理時間が見えにくくなります．

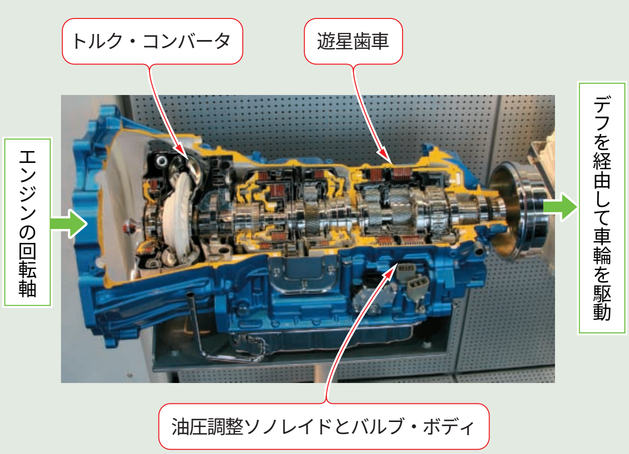
とくに，従来の衝突検知型通信（CSMA/CD；carrier sense multiple access with collision detection）で信号を取り込むとワーストケースが確定せず，「万が一，信号が遅延したら」といった処理をどんどん加えることになり，ソフトウェアの複雑性を助長してしまいます．

最近注目されているFlexRay通信はタイム・トリガ方式と呼ばれ，あらかじめ設計したタイム・スケジュールにのっとって信号転送が行われるため，ワーストケース処理時間を計算できます．このタイム・トリガ方式ということばは，自動車分野でブームのようになっています．すでに制御ソフトウェアの処理周期を一定時間にするなど，タイム・トリガ的思想が織り込まれてきていますが，この傾向はますます拡大すると思われます．

column　システム開発者のためのメカ用語解説

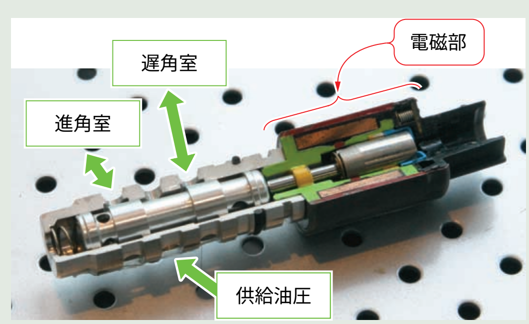
エレクトロニクス関連に携わっているエンジニアの中には，自動車の機械的機構に関する用語を聞いてもピンと来ない方もいることでしょう．ここでは，本文中に出てきたこうした用語を簡単に説明します．

- **イグナイタ**――日本語では「点火装置」．混合気を圧縮したものに着火するため，数万Vの火花を出す．ケタリング方式は，イグニッション・コイル（昇圧のためのコイル）の1次コイルの断続を接触型のポイント接点で行っている（接点不良などの不ぐあいが発生しやすい）．現在主流のフル・トランジスタ方式は，1次コイルの断続を非接触型のセンサ・スイッチにしたもの．
- **インジェクタ**――日本語では「燃料噴射装置」．電子制御により点火の際に燃料を噴射する．キャブレタから置き換わった．
- **オートマチック・トランスミッション（AT）**――日本語に訳すと「自動変速装置」．本文でも述べたとおり当初は油圧式だったが，最近ではほとんどが電子制御化されている．エンジン（トルク）のパワーを有効に使うため，変速の段数を増やす傾向にある（**写真A-1**）．多段化することで燃費が向上し，乗りごこちも良くなる．
- **サスペンション**――日本語では「懸架装置」．路面からの振動や衝撃などを和らげる装置．
- **ショック・アブソーバ**――サスペンションの動きを減衰するもの．走行状態に応じて減衰力を可変にできるものもある．
- **スタビライザ**――車の横揺れを抑えるもの．
- **ディストリビュータ**――点火系統において高圧を配電するための装置．4気筒，6気筒などと呼ばれるエンジンの各燃焼室に備えられたプラグに順番に火花を配電する．
- **負圧吸引式キャブレタ**――日本語では「気化器」とも呼ばれる．燃料（ガソリン）と空気を混ぜて適切な混合気をつねに生成し，エンジンの燃焼室に送り込む装置．
- **リニア・ソレノイド**――電気信号を機械的な直線運動に変える部品．油圧制御などに用いられる（**写真A-2**）．バルブの開閉を連続的に制御できるので，エンジンの高回転から低回転まで幅広く対応できる．



写真A-1　ATの例

写真はアイシン精機の小型トラック（バス）用6速オートマチック・トランスミッション（AT）の断面



写真A-2　リニア・ソレノイドの例

写真はVVT（variable valve timing）用のリニア・ソレノイドの断面

大規模ソフトウェアになっていくと，より効率的な実装および検証が必要になります．実装と検証を効率的に行うもっとも有効な手段は，（冗談抜きに）「新たにソフトウェアを作らないこと」です．つまり，ソフトウェアを部品化し，再利用することです．

ソフトウェアの再利用は古くて新しい永遠のテーマです．実際にソフトウェアを部品化して再利用するため，ソフトウェア・プラットホームを標準化していく動きが各方面で活発に行われています．自動車分野では，欧州の自動車メーカが中心となって立ち上げた「AUTOSAR」や国内の自動車メーカが中心となって設立した「JasPar」がその目的で活動しているといわれています．より効果的で標準的なソフトウェア・プラットホームが一般的になることが期待されています．

検証の容易さ，複雑性の低減という面では，大規模ソフトウェアをどう切り分けて検証できるかがキーとなります．また，先述の「機能安全」というキーワードでいうと，ソフトウェアの実装や検証の信頼性に対する要求の厳しさは，目的とされる車の機能によりレベルが異なるSIL（Safety Integrity Level）と呼ばれる安全度要求水準で考える，という手法が今後広まると言われています．大規模かつ統合化された，SILの異なる各機能ソフトウェアを効率的に検証していくためにも，各機能を影響なく分離実装できるソフトウェア・プラットホームが必要と思われます．時間保護機能やメモリ保護機能を搭載したリアルタイムOS装備の標準プラットホームの整備が待ち望まれます．

● 形式的検証手法の導入口としてのモデル・ベース

ソフトウェアの大規模化に伴い，テストを行っても，カバレッジを向上する工数は膨大になります．こうした背景から，数学的，形式的な検証手法であるフォーマル・メソッド（formal method）による検証の補完が以前から期待されています．

実際に機能安全規格「IEC61508」では，SILによってはフォーマル・メソッドの利用が強く推奨されています．とは言っても，前述したように，自動車制御の対象はハイブリッド・モデルです．そのため，モデリングが複雑で形式的検証が実施しにくい状況です．また，フォーマル・メソッドそのものの実用化課題もいまだに少なくありません．そのため，フォーマル・メソッドの現実的アプローチとして，例えばアーキテクチャ・レベルまでは形式的記述（モデル・ベース）を適用し，機能レベルからは従来のC言語などの構成を併用する方策などが検討されています．その場合，C言語で記述したソフトウェアはインターフェースを明確にして部品化し，検証を終えたら改修しないといったことの徹底が必要です．

モデル・ベース設計は，このフォーマル・メソッドをわかりやすく応用する導入口として期待されています．

● 機能安全では「ソフト・ハード協調設計」を要求

これまでに何度も「機能安全（または機能安全規格IEC61508）」というキーワードが出てきましたが，この考えかたでは「設計段階として，まず系全体のアーキテクチャ設計を行いなさい」と規定しています．その後，ハードウェア設計，ソフトウェア設計へと分かれていきます．つ

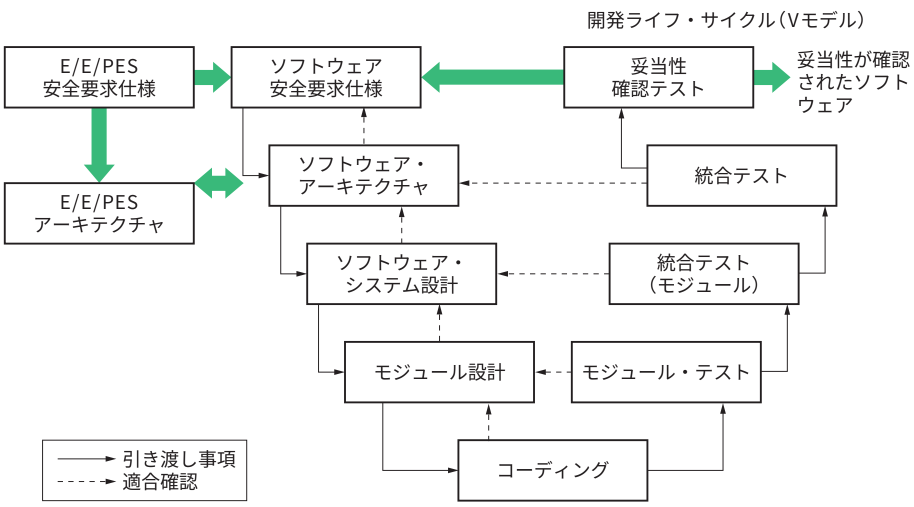


図8
IEC61508が規定する開発プロセス(14)
IEC61508は，開発プロセスをVモデルと規定している．図は，電気・電子・プログラマブル電子安全関連系（E/E/PES）のソフトウェア実現の例

まり，ソフトウェアとハードウェアを区別しないアーキテクチャ設計手法を推奨しています(図8).

ここで言うアーキテクチャ設計手法とは，「システム記述言語のC」などではなく，もっとアーキテクチャ寄りの「フォーマルなアーキテクチャ記述」という表現が適当です．先のアーキテクチャ記述言語ADLが注目されているのはこうした理由からです．ADL概念の進展は，ソフトウェア・ハードウェア協調設計も促進するものと期待されます．

4 車載ソフトウェア開発者に必要な知識

車載ソフトウェア開発者に求められる知識やスキルは，基本的には組み込みソフトウェア開発の知識と差はないと思います．ただし，上述したように使用される環境などの特殊性を考えると，次のようなポイントが期待されていると思います．

- 大規模化に伴い，ソフトウェアの工学的設計力や多人数開発におけるマネージメント力
- ハード・リアルタイムの世界なので，時間制約やメモリ制約に対処する経験
- ノイズ除去のためのフィルタ理論のほか，フィードバック理論や最近では数学モデルのソフトウェア実装経験
- システムやセンサ，アクチュエータや油圧の特性の把握(これがより良い制御ソフトウェアを生み出すためのかぎ)．現代制御理論を理解し，駆使できる技術者はひっぱりだこ
- グローバルなビジネス協業へ向けたグローバル・スタンダードの理解と実践
- 品質管理システムISO9000(今はISO16949)の理解と実践
- CMM(Capability Maturity Model)的ソフトウェア・プロセスの実践(今後はISO15504ベースのAutomotive SPICEやTPI-Automotiveなど，欧州の動向が注目されている)
- MISRA-Cコーディング規約やソース・コード・メトリックス分析の実践

● 機能安全規格IEC61508的共通思考が求められている

最後に，何度もキーワードで挙げた「機能安全規格IEC61508」についてお話しします．

車載ソフトウェアを安全にかかわる製品へ組み込むケースは多く，ソフトウェアが大規模になるに従い，設計や検証により注意を払うようになりました．会社や国をまたいだ共同作業やソフトウェア部品の再利用が進む中，安全設計に関するグローバルな指針があることで，相互理解を助け，品質が見えやすくなると期待されます．

機能安全国際規格IEC61508は「電気・電子・プログラマブル電子安全関連系(E/E/PES)の機能安全」と呼ばれ，システムを構成する全要素(メカ，センサ，ハードウェア，ソフトウェア)を対象とし，遵守すべきプロセスや技法を規定したものです．1998年から2000年にかけて制定されましたが，すでにJISでも規格化されています(JIS C0508)．安全に関する規格には，機械安全のISO12100，軍事産業ではDo178があります．IEC61508はプログラマブル電子安全系，つまりマイコン応用製品を対象とし，ソフトウェア要求事項を規定していることから，組み込み機器の分野では標準的になると注目されています．

IEC61508は7部から構成されています(図9)．具体的ではあるものの，「概念規格」とも言われ，適用領域でそれぞれサブ規格の制定が進められています．自動車分野ではISO26262として検討されています．

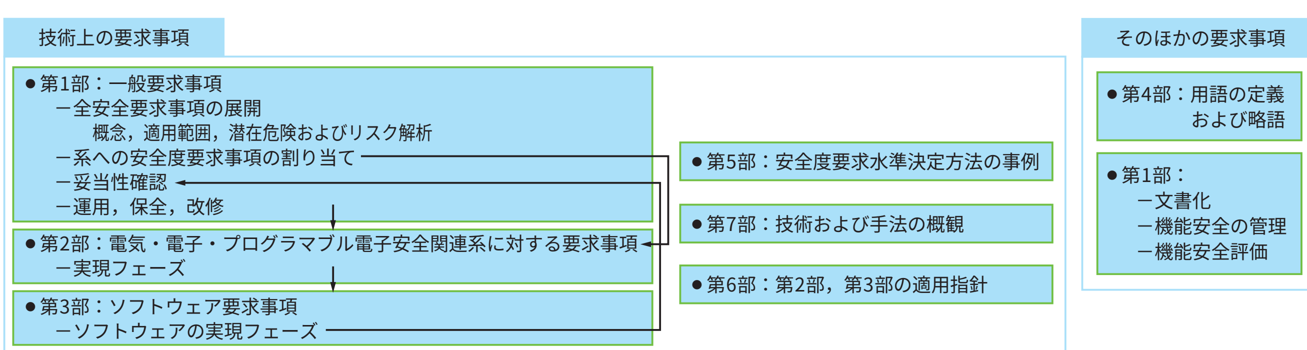


図9　IEC61508(6)

機能安全規格IEC61508は7部から構成されている．この中では，技術上の要求事項とそのほかの要求事項についての規定があるが，技術上の要求事項に多くを割いている

IEC61508の考えかたは，リスクを考慮した安全度要求水準で製品をレベル分けします．このレベルは前述のSILと呼ばれるもので，1～4の段階が設けられています（**図10**）．SILは1ランク上がるごとに信頼性がおよそ1けた上がることが想定されています（SIL4がもっとも要求水準が高くなる）．各レベルに応じて安全設計に関する各種の推奨技法が提示されています．推奨技法の数は，SIL1では16，SIL2では26，SIL3では42，SIL4では56と，かなり詳細に規定されています（**表1**）．

IEC61508は，開発プロセスをVモデルと定めています．さらに，そのVモデル内部のソフトウェア開発工程段階を具体的に規定しています．その各工程で必要な推奨技法をSILごとに規定しており，各前後工程の引き継ぎ事項や引き渡し事項が明確に共通認識できるという特徴があります．ただし，実施においてはどういった組織モデルや品質管理システムを採用するのかなどが影響してきます．各分野の具体的なサブ規定が要求される要因の一つです（**図11**）．

● 機能安全によって何が変わるのか

本稿でお話ししてきた大規模ソフトウェアの開発に必要とされる，実施されている技法や期待されている技法は，実はほとんどIEC61508で要求されているものです．その意味で最近話題になる技法（例えばフォーマル・メソッドやコーディング規約）は，IEC61508への関心の表れでもありますし，逆に大規模ソフトウェアを効率的に，かつ安全に開発していくには実際に必要な手法の体系であるともいえます．

機能安全IEC61508は製品単位で認証を取得します．そのプロセスの範ちゅうは製品を構成するシステム，ハードウェア，ソフトウェア，半導体の設計にかかわる方が関連します．したがって，ソフトウェア開発工程だけでなく，上流からの要件定義，管理から製品開発全体の関連技術が必要です．

機能安全IEC61508の考えかたが広まるのはまだ先のよ

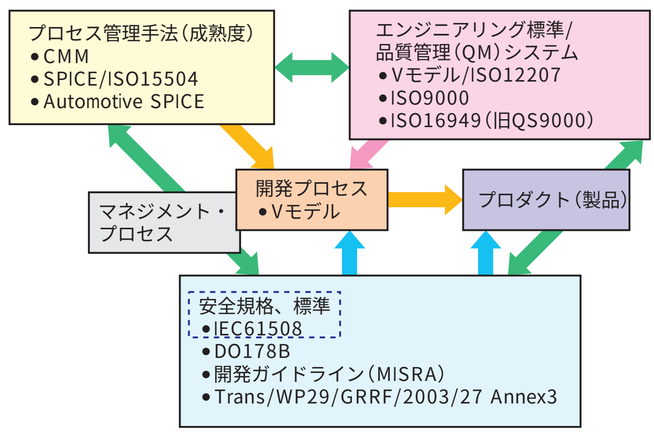


図11　製品と開発プロセスに影響する，タイプの異なる標準

大規模ソフトウェアの開発に必要とされる，実施されている技法や期待されている技法は，実はほとんどがIEC61508で要求されているものである

▶ 表1
推奨技法の例
推奨技法の数は，SIL1では16，SIL2では26，SIL3では42，SIL4では56と多い

SIL（安全度要求水準）→

	技術/手法	SIL1	SIL2	SIL3	SIL4
安全要求仕様アーキテクチャ設計	コンピュータ支援仕様ツール	R	R	HR	HR
	故障検出および診断	R	R	HR	HR
	エラー検出およびコード修正	R	R	R	HR
	異常断定プログラム	R	R	R	HR
	動的再コンフィグレーション	―	NR	NR	NR
プログラム言語	強固に形式化されたプログラム言語	HR	HR	HR	HR
	言語サブセット	―	―	HR	HR
	証明付きツール	R	HR	HR	HR
	検証済みソフトウェア・モジュール	R	HR	HR	HR
詳細設計	構造プログラム	HR	HR	HR	HR
	設計およびコード化規格	R	HR	HR	HR
機能安全評価	複雑度測定基準	R	R	R	R
	異常ツリー分析（FTA）	R	R	HR	HR
	異常モード効果臨界分析（FMEA）	R	R	HR	HR
半公式試験	機能ブロック・ダイアグラム	R	R	HR	HR
	有限状態遷移図	R	R	HR	HR
	タイム・ペトリネット	R	R	HR	HR
モジュラ・アプローチ	サブルーチンの一つのENTRY/EXIT	HR	HR	HR	HR
	カプセル化	R	HR	HR	HR

HR：強く推奨，R：推奨，NR：非推奨

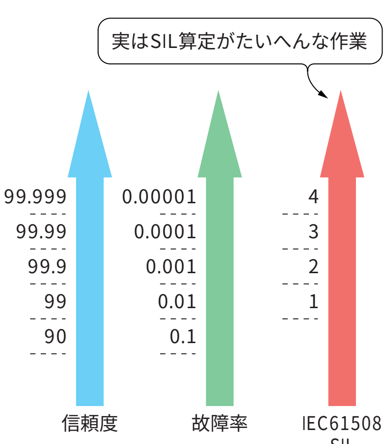


図10　故障とSIL[6]

SILは安全度要求水準のことであり，1～4のレベルに分けられる

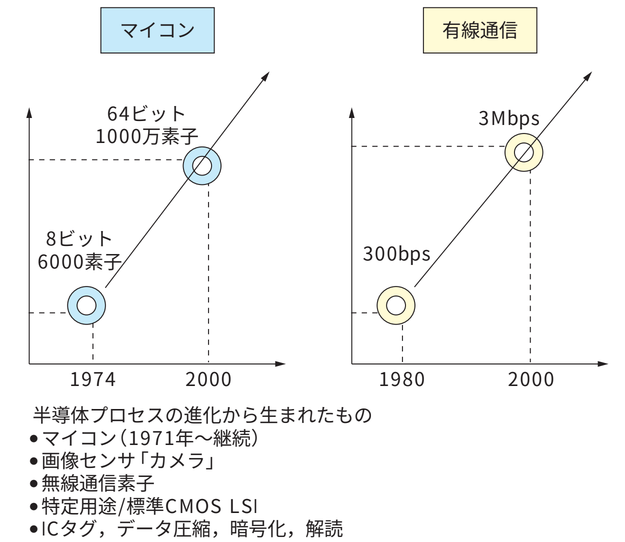


図12　マイコンの革新に支えられる車載システム

18ヵ月でシリコン・チップの集積度は2倍になるというムーアの法則にのっとって，マイコンの革新が進められてきた．1チップのLSIで実現できる機能は継続的に高機能化，低コスト化していく

うに理解されている方もいると思います．一方で，例えば公共施設の発注要件などで機能安全に基づく要求が世界では広がっているとも言われています．PLC(programmable logic controller)と呼ばれる工作機械に利用されるコントローラについては，欧州ではメーカ各社が2003年にSIL3の認定を受けたsafety-PLCの販売を一斉に開始しています．

グローバルな考えかたを身につけ，対応していくことは，国際的な分業や競争が拡大する中，重要視されるので，それらの手法に精通する人材がより必要とされています．

● これからの自動車は，「知能化」，「ロボット化」

自動車の進化はマイコンの革新に支えられている，と言っても過言ではありません．マイコンの革新は，ムーアの法則にのっとって過去35年間，永続的に進化しました．今後もしばらくはこの法則が崩れそうにありません(**図12**)．

自動車は，大型電源を自己保有しているため，高度な制御を実現する高速マイコンを搭載しやすく，移動可能であるという特性から，夢のロボット的特性が発現しやすい環境と期待されます．ここでロボットとは，一般に目的とする操作や作業を自動的に，かつ自律的に行うことのできる機械を指します．また，知能ロボットは人工知能によって行動を決定できる，人に近い形および機能を持つ機械といえます．ですが，筆者は「対話(操作)する人を知的に把握・判断し，高度な反応や行動で情緒的なまでの満足感を得られる機械」であるとも考えています．

今まで築き上げられた車の基本制御の電子化をもとに，エレクトロニクス，とくにソフトウェア技術の革新によって，今後，車は車両総合制御からさらにITS化，ロボット化が実現されていくものと期待されています．

参考・引用*文献

(1) 電気学会・42V電源化調査専門委員会；自動車電源の42V化技術，オーム社，2003年．
(2) 新誠一；カーエレクトロニクス最前線，工業調査会，2006年．
(3) 鈴木和幸ほか；正しい故障・信頼性解析で事故を防げ！ トラブルを回避せよ！，機械設計，2005年10月号，pp.11-41.
(4) 進藤智則；ソフトウェアは硬い，日経エレクトロニクス，2005年12月19日号，pp.87-121.
(5) 進藤智則，山田剛良，大槻智洋；価格下落を糧に世界を獲る「多品種大量」，日経エレクトロニクス，2006年4月24日号，pp.77-110.
(6)* 鈴村延保；車載コンピュータにおけるソフトウェア信頼性技術の動向と背景，JASA/CESTセミナ，2005年10月．
(7) 産業技術総研；機能安全規格と適合認証，産総研ワークショップ，2006年2月．
(8) 吉岡律夫；第3の波「機能安全」，日刊工業新聞，2005年2月7日．
(9) 羽生田栄一；OOPSLA99報告，OGIS総研．
(10) 青山元男；カー・メカニズム・マニュアル[ベーシック編]，ナツメ社，1991年．
(11) 社団法人自動車技術会のホームページ；http://www.jsae.or.jp/
(12) SAE(Society of Automotive Engineers)のホームページ；http://www.sae.org/
(13) 宮崎技術研究所のホームページ；http://miyasan.serio.jp/series4/densi0921.html(電気と電子のお話)
(14)* 機能安全に関するWebサイト；http://systemsafety.fc2web.com/，http://www.sipi61508.com/
(15) AUTOSARのホームページ；http://www.autosar.org/
(16) JasParのホームページ；https://www.jaspar.jp/
(17) ADL概念に関するWebサイト；http://www.ogis-ri.co.jp/otc/hiroba/others/OOPSLA99/pdf/OOPSLA99report.pdf(Is UML ADL?)
(18) DSLに関するWebサイト；http://www.adapdev.com/blogs/smccormack/PermaLink,guid,67459107-3232-41e6-9d53-7ed4027f0501.aspx(UML or DSL?)
(19) Automotive SPICEのホームページ；http://www.automotivespice.com/

すずむら・のぶやす
アイシン精機(株)

<筆者プロフィール>
鈴村延保．1977年，広島大学工学部を卒業．アイシン精機にて，自動変速機やアクティブ・サスペンション，ABS，VSC用のコンピュータとそれに関連するICの開発・製品化に従事．